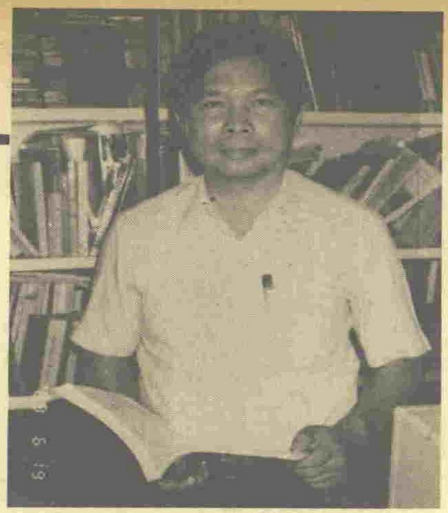
นานาทัศนะ ไวรัสคอมพิวเตอร์

กองบรรณาธิการ

หลายคนคงจะเคยได้ยินคำว่า "ไวรัสคอมพิวเตอร์" มาบ้างแล้ว เนื่องจากชื่อเสีย (ง) อันเลื่องลือในความประพฤติที่ไม่ชอบมาพากลของโปรแกรมตัวนี้ ด้วยลักษณะของโปรแกรมชนิดนี้ที่มีความสามารถเลียนแบบการกระทำของสิ่งมีชีวิตในการจำลองตัวเองได้ และซ่อนตัวลงในสื่อกลาง เช่น ดิสเกตต์ ฮาร์ดดิสก์ ได้อย่างเงียบ ๆ เพื่อรอโอกาสและจังหวะที่จะแสดงความสามารถในการทำลาย หรือก่อความรำคาญออกมาตามความคิดของนายผู้สร้างมัน ผลที่ตามมาก็คือ ทำให้เกิดความเสียหายต่อบุคคลและส่วนรวม โดยที่จะต้องมาแก้ไข และหาวิธีป้องกันในส่วนงานของคนที่เกี่ยวข้องกับคอมพิวเตอร์ ซึ่งจะก่อให้เกิดการเสียเวลาและแรงงานในเรื่องที่ไม่น่าจะเกิดขึ้นดังกล่าว จากผลงานที่ผู้สร้างไวรัสคอมพิวเตอร์ได้กระทำขึ้นนี้ ทำให้เกิดการเคลื่อนไหวต่อผู้ที่ใช้และเกี่ยวข้องกับคอมพิวเตอร์ในบ้านเรา ดังนั้น เพื่อที่จะให้ผู้อ่านได้ทราบถึงลักษณะของไวรัสคอมพิวเตอร์ และสถานการณ์ของการระบาดในปัจจุบัน ทางกองบรรณาธิการจึงขอนำท่านผู้อ่านไปสัมผัสกับบุคคลจากหน่วยงานต่าง ๆ ที่เกี่ยวข้องกับคอมพิวเตอร์ในบ้านเรา ตามลำดับดังต่อไปนี้



ดร.ครรชิต มาลัยวงศ์

แผนกวิทยาการคอมพิวเตอร์
สถาบันเทคโนโลยีแห่งเอเชีย (AIT)

ไมโคร ไวรัสคอมพิวเตอร์ในความคิดเห็นของคุณครรชิตนั้นเป็นอย่างไรบ้าง

ดร.ครรชิต ผมคิดว่าไวรัสนี้เป็นเรื่องที่สำคัญมากต่อศูนย์คอมพิวเตอร์ เรื่องของข้อมูลในระบบคอมพิวเตอร์ ถ้ามามองในแง่ของนักคอมพิวเตอร์มือสมัครเล่น ผลกระทบมันอาจจะไม่มากนัก แต่ถ้าเผื่อเรามองการใช้คอมพิวเตอร์ในหน่วยงาน บริษัท ห้างร้าน ธนาคาร ผลกระทบของไวรัสจะมีมาก โดยเฉพาะข้อมูลหรือโปรแกรมที่สำคัญของหน่วยงานราชการ ไวรัสจะทำความเสียหายได้อย่างมาก เพราะฉะนั้นก็มีปัญหาอยู่ว่า ทำอย่างไรเราจึงจะป้องกันเรื่องนี้ให้ได้ผลเต็มที่ ซึ่งเป็นเรื่องค่อนข้างยาก เพราะไวรัสเป็นโปรแกรมซึ่งมีคนทำขึ้น และคนที่ทำโปรแกรมไวรัสอาจจะดัดแปลงได้ต่าง ๆ นานา มันไม่มีวิธีเดียวที่จะทำได้แบบแปลก ๆ วิธีป้องกันก็ค่อนข้างยาก ถ้าจะทำฮาร์ดแวร์มาป้องกันหรือซอฟต์แวร์มาป้องกันอาจจะป้องกันได้เพียงแบบเดียว หรือประเภทเดียว หรือพวกที่มีพฤติกรรมแบบเดียวกัน พอมันเปลี่ยนพฤติกรรมหรือวิธีการเป็นแบบอื่นมันก็คงจะยากที่จะป้องกันได้ ผมคิดว่ามันก็เหมือนเชื้อโรคทั่วไปนั่นแหละ มันอาจจะมีเชื้อโรคหวัด ปวดท้อง หรืออื่น ๆ ดังนั้นยาที่ใช้แก้ก็แก้ได้ประเภทเดียว วิธีการป้องกันไวรัสคอมพิวเตอร์ก็เช่นเดียวกัน ถ้าเผื่อมันเป็นซอฟต์แวร์ที่ผลิตออกมาใหม่แหวกแนวที่เราเคยเห็น เราก็อาจป้องกันมันไม่ได้ เพราะฉะนั้นเราจึงน่าจะดูวิธีการป้องกันในเชิงจัดการ เช่น เรากำลังวิตกกังวลอยู่ในเรื่องของบริษัทหรือหน่วยงาน เพราะฉะนั้นบริษัทหรือหน่วยงานจะต้องมีมาตรการในเชิงจัดการที่จะมาป้องกันไวรัส อย่างเช่น มีระเบียบวิธีการแน่ชัดในการที่จะนำซอฟต์แวร์เข้าสู่บริษัท การนำดิสเกตต์เข้าสู่บริษัท ดิสเกตต์เหล่านั้นจะต้องผ่านการซื้อมาอย่างถูกต้องเชื่อถือได้ วิธีการป้องกันจะได้ผลหรือไม่ขึ้นอยู่กับวิธีการที่จะตรวจสอบดูแลพนักงานให้ทำงานกันไปตามกฎเกณฑ์นั้น ยกตัวอย่าง กฎเกณฑ์ห้ามนำดิสเกตต์วางไว้บนโต๊ะ ทุกอย่างต้องอยู่ในลิ้นชัก ก็ต้องทำไปตามนั้น จะต้องมีเจ้าหน้าที่คอยดูว่าไม่มีการวางดิสเกตต์ไว้เรี่ยราด หรือหลังจากชั่วโมงการทำงานแล้วทุกคนจะต้องบันทึกชื่อดิสเกตต์ที่ใช้ต่าง ๆ เพื่อป้องกันการนำดิสเกตต์อื่นเข้ามา หรือนำดิสเกตต์จากสำนักงานออกไปนี้เป็นตัวอย่างของการจัดการ วิธีการจริง ๆ นั้นอาจแตกต่างกันออกไป ขึ้นอยู่กับสิ่งแวดล้อมที่แตกต่างกันไป เช่น เป็นระบบการสื่อสาร ไวรัสก็อาจเข้ามากับระบบการสื่อสารนั้นได้ ไม่จำเป็นต้องมาจากดิสเกตต์เท่านั้น เพราะฉะนั้นต้องมีกฎเกณฑ์ต่าง ๆ ในการควบคุมการใช้การสื่อสาร การที่เราใช้มาตรการเข้มงวดและจริงจังก็จะสามารถป้องกันไวรัสที่จะแทรกซึมเข้ามาในหน่วยงานได้ จากที่กล่าวมานี้มาจากสมมติฐานที่ว่าไวรัสมาจากบุคคลภายนอกที่ไม่หวังดี หรือโดยอุบัติเหตุหรือโดยบังเอิญ คิดว่ามาตรการทางด้านจัดการสามารถช่วยได้มาก ถ้าเป็นไวรัสที่คนภายในเราทำขึ้นเองก็เป็นเรื่องที่ป้องกันได้ยาก ไวรัสเป็นโปรแกรมและมันเป็นเรื่องที่น่าท้าทาย เพราะฉะนั้นก็อาจจะมีคนที่สนใจทำไวรัสขึ้น ผมมีความเชื่อว่าเด็กของเราหรือนักโปรแกรมเมอร์ของเราอยู่ในวิสัยที่จะทำได้ โดยเฉพาะถ้ามีการสังเกตการทำงานของไวรัสบางตัว หรืออ่านตำราต่าง ๆ ที่เขียนเกี่ยวกับเรื่องไวรัส ก็สามารถทำไวรัสเองได้ ซึ่งถ้าพบคนที่ชอบท้าทาย ลองดีแบบนี้ก็อาจจะคิดทำไวรัสขึ้นมาในสำนักงานหรือหน่วยงานนั้น การป้องกันก็ทำได้ยากขึ้น การป้องกันจะไม่ได้อยู่กับการจัดการเพียงอย่างเดียว แต่ต้องขึ้นอยู่กับจริยธรรม คือต้องมีการอบรมเชิงจริยธรรมว่าการทำงานแบบนั้น อาจจะเป็นเรื่องที่ท้าทายปัญญา ความสามารถ แต่มันไม่ถูกต้องในเชิงของจริยธรรม และจะก่อให้เกิดปัญหาตามมาอีกมากมาย

ในแง่ของผู้บริหารต้องอยู่ภายใต้กฎเกณฑ์ที่ตั้งไว้ด้วย แต่บางครั้งผู้บริหารเองก็ไม่ทำตัวอยู่ภายใต้กฎเกณฑ์ เช่น ห้ามเอาดิสเกตต์เข้ามาก็นำเข้ามา อันนี้จะต้องใช้วิธีการทางด้านการฝึกอบรมให้เข้าใจผลกระทบอย่างรุนแรงที่เกิดจากไวรัสคอมพิวเตอร์ ซึ่งสิ่งนี้จะส่งผลไปในอนาคต เนื่องจากผู้บริหารอาจจะใช้เครื่องประเภทแลปท้อป มีการนำข้อมูลจากที่บ้านมาสำนักงานหรือจากสำนักงานไปบ้าง ก็จะได้หาวิธีการป้องกันไวรัสไม่ให้เข้าไปยุ่งในระบบการทำงานของเครื่องได้

ไมโคร การตรวจสอบว่าระบบงานของเราติดไวรัสคอมพิวเตอร์หรือไม่ ควรทำอย่างไร

ดร.ครรชิต ถ้าเป็นไวรัสที่รู้อยู่ว่ามันเข้าเครื่องแล้วมันจะไปแก้ไขดัดแปลงส่วนใดส่วนหนึ่งในหน่วยความจำ หรือในดิสเกตต์ ฉะนั้นเราจะใช้คุณสมบัติดังกล่าวเหล่านั้นคอยตรวจสอบว่า เนื้อที่ในดิสเกตต์ของเราหรือในหน่วยความจำของเราถูกเปลี่ยนแปลงไปโดยไม่ชอบมาพากลหรือเปล่า สิ่งที่ต้องศึกษาก็คือ เครื่องปกติแล้วแผนที่ของหน่วยความจำเป็นอย่างไร แผ่นที่ของดิสเกตต์เป็นอย่างไร เวลามันทำงานมันเริ่มทำอะไรก่อนอะไรหลังซึ่งเป็นเรื่องกว้าง ๆ ทั่ว ๆ ไป จากนั้นเราก็เอาจุดนั้นมาทำการตรวจสอบ เมื่อไวรัสเข้าสู่เครื่องสิ่งที่มันจะโจมตีก่อนก็คือจุดที่เป็นแผนที่ของหน่วยความจำ มันจะย้ายตำแหน่งโปรแกรมต่าง ๆ เพื่อจะให้มันแฝงตัวอยู่ได้ ถ้าเผื่อหน่วยงานหนึ่งไม่มีเจ้าหน้าที่ซึ่งมีความรู้ความสามารถทางด้านฮาร์ดแวร์ หรือซอฟต์แวร์ที่จะบอกได้อย่างนั้น ก็คงจะต้องหันไปอาศัยโปรแกรมตรวจสอบ และทำลายไวรัส เช่น โปรแกรมวัคซีน โปรแกรมศิริราช เป็นต้น มาทำการตรวจสอบแผนที่ของหน่วยความจำ (โปรแกรมส่วนใหญ่จะทำอย่างนั้น) ว่ายังเหมือนเดิมหรือไม่ แต่ในเชิงของผู้ใช้โดยทั่วไปจะสังเกตได้อย่างไร ถ้าไม่มีโปรแกรมในการตรวจสอบ ซึ่งเรื่องนี้อาจจะดูจากอาการต่าง ๆ แทน เช่น เครื่องเคยทำงานเร็วกลับช้าลง โปรแกรมมีลักษณะอาการแปลก ๆ พิมพ์ตัวอักษรแปลก ๆ ออกมา หรือเวลาสั่งโปรแกรมให้ทำงานแล้วไม่ทำ นอกจากนั้นทุกครั้งที่เราใช้ดิสเกตต์ ควรสังเกตว่าไฟล์ของเรามีขนาดเท่าไร มีอะไรอยู่บ้าง ก่อนใช้ควรตรวจสอบดูว่าดิสเกตต์นั้นมีลักษณะเหมือนเดิมหรือไม่ มีไฟล์พิเศษเพิ่มเติมเข้ามาหรือไม่ ทำให้เนื้อที่ในดิสเกตต์หายไปหรือไม่

รศ.ยืน ภู่วรวรรณ

หัวหน้าห้องปฏิบัติการวิจัย
ไมโครคอมพิวเตอร์คณะวิศวกรรมศาสตร์
มหาวิทยาลัยเกษตรศาสตร์

ไมโคร สาเหตุของการเกิดมีไวรัสคอมพิวเตอร์ขึ้นนั้นมาจากสิ่งใด

รศ.ยืน สาเหตุจากเทคโนโลยีเปิด กล่าวคือทุกคนมีสิทธิที่จะเรียนรู้สิ่งต่าง ๆ ได้มากขึ้น รู้ว่าระบบงานของเครื่องทำงานอย่างไร เรารู้ตั้งแต่โครงสร้างของฮาร์ดแวร์เป็นอย่างไร ไบออสไปควบคุมอะไรในฮาร์ดแวร์ สั่งอะไรไปประสานกับโอเอสโอเอสจัดการเรื่องอะไร มีฟังก์ชันของโอเอสทำอะไรบ้าง ฟังก์ชันส่วนนี้มีการแอพพลิเคชั่นอะไรได้บ้าง นี่เป็นสาเหตุหนึ่งที่ทำให้เกิดมีโปรแกรมไวรัสขึ้นมา

ไมโคร หลักการทำงานของไวรัสและการแพร่ของไวรัสมีอย่างไรบ้าง

รศ.ยืน ตัวโปรแกรมไวรัสคอมพิวเตอร์โดยหลักการสำคัญต้องเป็นตัวพาหะได้ ตัวเองเป็นพาหะที่จะส่งต่อไปให้คนอื่นได้ สมมติเครื่องคอมพิวเตอร์เครื่องหนึ่งเป็นตัวพาหะนำเชื้อ มันก็จะต้องพยายามแพร่เชื้อไปให้คนอื่น โอกาสที่มันจะแพร่เชื้อไปได้มี 2 ทาง คือ ทางดิสเกตต์ที่นำเอาไป และทางการสื่อสารข้อมูลที่ต่อถึงกัน

โปรแกรมไวรัสจะติดต่อได้ มันต้องแฝงอยู่ในตัวกลางอะไรสักอย่างหนึ่ง เช่น ในดิสเกตต์ แล้วจากนั้นมันก็จะพยายามเข้าไปอยู่ในหน่วยความจำของเครื่อง พร้อมที่จะแพร่เชื้อตัวมันเองไปยังดิสก์แผ่นอื่น และดิสก์แผ่นนั้นก็จะเป็นพาหะนำเชื้อต่อไปยังเครื่องอื่น

ไมโคร ไม่ทราบว่าไวรัสคอมพิวเตอร์ที่พบมีตัวไหนบ้าง

คุณเอนก ไวรัสที่พบมี (c) BRAIN, 1K, YEIPP, sUMs-Dos , FATERASER และ T-2

ไมโคร มีไวรัสคอมพิวเตอร์ตัวไหนที่เขียนขึ้นมาเพื่อการทำลายข้อมูลโดยตรงบ้าง

คุณเอนก FATERASER น่าจะเป็นตัวที่เขียนมาเพื่อจุดมุ่งหมายในการทำลายข้อมูลโดยตรง

คุณเอนก ศิรจริยาวิภิวัฒน์

ผู้ช่วยนักวิจัยโครงการวิจัย และพัฒนา
เครื่องต้นแบบคอมพิวเตอร์ 32 บิต
มหาวิทยาลัยเกษตรศาสตร์

ไมโคร ไม่ทราบว่าจะมีวิธีการป้องกันไวรัสคอมพิวเตอร์อย่างไรบ้าง

คุณเอนก วิธีป้องกันที่ทำได้คือ แผ่นดิสค์ควรปิดแผ่นป้องกันการเขียนทุกแผ่น ถ้าเป็นฮาร์ดดิสค์ ต้องมีการตรวจสอบการใช้งานโดยใช้รหัสผ่าน แต่ก็มีโอกาสติด และไม่ควรใช้เครื่องต่อจากคนอื่นโดยไม่ปิดเครื่องเสียก่อน

ไมโคร แนวโน้มของการติดไวรัสคอมพิวเตอร์ในปัจจุบันจะเป็นอย่างไร

รศ.ยืน ในปัจจุบันการติดไวรัสจะสูงขึ้นเรื่อย ๆ เพราะโครงสร้างของไวรัสจะทำให้ง่ายต่อการติดมากขึ้น ติดแล้วบางทีก็ไม่รู้ตัว ไม่แสดงอาการ ถ้าตัวหลัง ๆ ที่ทำขึ้นกลบดานอะไรบางอย่างไว้ โดยที่ไม่แสดงอาการอะไรเลย ให้มันแพร่ไปมาก ๆ แล้วค่อยแสดงอาการออกมา การป้องกันในกรณีนี้คงทำได้ยากขึ้น

ไมโคร จุดประสงค์เริ่มแรกของการสร้างโปรแกรมไวรัสเพื่ออะไร

รศ.ยืน จริง ๆ แล้วจุดประสงค์เริ่มต้นไม่ใช่สร้างมาเพื่อการทำลาย แต่เพื่อทำหน้าที่ก๊อบปี้ตัวเองไปในสายแลนด์ คอยเช็คตัวเซ็นเตอร์ว่าตอนนี้แลนด์ต่อถึงไหนบ้าง ถ้าอันไหนไม่ต่อก็จะก๊อบปี้ตัวเองเข้าไปในสายแลนด์นั้น เพื่อทำหน้าที่คล้าย ๆ โอเอส ต่อมามีคนเขียนเกมขึ้นมาสองโปรแกรมใส่ลงในหน่วยความจำ แล้วให้ไล่กินกัน ดูว่าโปรแกรมใครจะหยุดทำงานก่อนกัน เป็นการประลองฝีมือกัน จากหลักการที่กล่าวนั้นได้มีผู้เปลี่ยนแปลงจนเกิดเป็นไวรัสคอมพิวเตอร์ที่มีลักษณะการทำงานเช่นในปัจจุบัน

ไมโคร สุดท้ายนี้ไม่ทราบว่าอยากจะฝากอะไรให้แก่ท่านผู้อ่านบ้าง

รศ.ยืน ถ้าเราเจอไวรัสตัวไหนไม่ควรเก็บมันไว้ พยายามทำลายมันให้หมด แล้วสักวันหนึ่งไวรัสต่าง ๆ จะหมดไปเอง

ดร.ปัญญา เปรมปรีดิ์

ผู้อำนวยการสำนักงานวางแผนและ
ปฏิบัติการคอมพิวเตอร์
ธนาคารแห่งประเทศไทย

ไมโคร ในแง่ความคิดเห็นของคุณปัญญานั้น ไวรัสคอมพิวเตอร์นั้นมีอันตรายอย่างไรบ้าง

ดร.ปัญญา ในความคิดของผมไวรัสคอมพิวเตอร์ไม่มีอันตรายมากนัก เพราะผู้สร้างไม่สามารถบีบหรือบังคับมันเพื่อสร้างผลประโยชน์ให้แก่ตนเองได้ มีแต่การทำลายอย่างเดียวไม่ได้ก่อให้เกิดประโยชน์ให้แก่ผู้ทำ ซึ่งไม่สามารถเปิดเผยตนเองได้ว่าเป็นผู้ที่คิดค้นและสร้างไวรัสคอมพิวเตอร์ขึ้นมา

ในแง่ของการทำลายนั้น ประเทศต่าง ๆ ที่เป็นคู่สงครามกัน อาจจะนำไวรัสคอมพิวเตอร์เข้ามาเป็นอาวุธที่สำคัญอันหนึ่งในการต่อสู้กันโดยปล่อยไวรัสคอมพิวเตอร์เข้าไปทำลายล้างระบบงานคอมพิวเตอร์ต่าง ๆ ของประเทศคู่สงคราม ทำให้

ประเทศคู่สงครามเกิดความเสียหายในด้านต่าง ๆ ซึ่งประเทศผู้นำไวรัสเข้าไปใช้นั้นได้มีการวางมาตรการป้องกันตัวเองไว้ก่อนแล้ว เพื่อไม่ให้ส่งผลกระทบเข้ามาสู่ตนเอง

แต่ผมมีความเป็นห่วงในเรื่องของการนำไวรัสคอมพิวเตอร์มาแกล้งกันในหน่วยงานต่าง ๆ ทั้งภาครัฐบาลและเอกชน หรือตามศูนย์คอมพิวเตอร์ต่าง ๆ โดยผู้ที่มีการขัดแย้งกันจะนำเอาไวรัสคอมพิวเตอร์มาปล่อยให้แพร่ระบาดเพื่อทำลายข้อมูลของฝ่ายตรงข้าม ผลที่เกิดขึ้นอาจทำการแก้แค้นผู้ที่ตนขัดแย้งได้ แต่ผลที่ตามมาอาจจะไม่กระทบกระเทือนแค่เพียงบุคคลที่ต้องการแก้แค้นคนเดียว อาจกระทบต่อหน่วยงานนั้นทั้งระบบ เมื่อไวรัสคอมพิวเตอร์แพร่กระจายไปยังบุคคลอื่นต่อไปอีก ซึ่งเรื่องนี้ผมคิดว่าน่าเป็นห่วงมาก ควรหาวิธีการป้องกันไว้ก่อน

อันที่จริงแล้วนั้นถ้าเราไม่ตื่นเต้นไปกับไวรัสคอมพิวเตอร์มากนัก ไม่ให้ความสนใจมากนัก ไวรัสคอมพิวเตอร์ก็จะค่อย ๆ เลือนหายไปเอง ถ้าเรายิ่งให้ความสนใจมันมากก็จะเป็นการกระตุ้นให้ผู้เขียนหรือผู้สร้างไวรัสคอมพิวเตอร์มีความอยากทดลองสร้างไวรัสตัวใหม่ ๆ ขึ้นมาอีก เพื่อทดสอบความสามารถของตนเองและทดสอบความรู้ของตนที่มีอยู่ ซึ่งการกระทำในลักษณะนี้ไม่มีผลดีต่อตนเอง เพราะไม่มีประโยชน์ต่อผู้อื่นมีแต่การทำลายมากกว่า

ไมโคร ไวรัสคอมพิวเตอร์ที่พบที่นี่มีชนิดใดบ้าง เข้ามาทางใด

ดร.ปัญญา ไวรัสคอมพิวเตอร์ที่พบมี (c) BRAIN 2 ครั้ง และอิสราเอลไวรัส 1 ครั้ง การแพร่กระจายเข้ามานั้นสันนิษฐานมาจากผู้นำโปรแกรมภายนอกที่มีไวรัสคอมพิวเตอร์มาใช้บนเครื่องคอมพิวเตอร์ของที่นี่ จึงทำให้เกิดการติดไวรัสคอมพิวเตอร์เกิดขึ้น แต่ก็ไม่ส่งผลกระทบอะไรมากนัก

ไมโคร ไม่ทราบว่าพอจะแนะนำวิธีการป้องกันไวรัสคอมพิวเตอร์อย่างไรบ้าง

ดร.ปัญญา การป้องกันนั้นโดยทั่วไปควรทำดังนี้

1. แผ่นฟลอปปี้ดิสค์ที่เป็นแผ่นดอส หรือโปรแกรมที่เราใช้งานอยู่เสมอ ๆ ควรปิดด้วยแผ่นป้องกันการเขียน ซึ่งจะป้องกันไม่ให้ไวรัสเข้าไปในแผ่นดิสค์นั้นได้

2. ถ้าทราบว่ามีโปรแกรมไวรัสคอมพิวเตอร์อยู่ในหน่วยความจำของเครื่องก็ให้ปิดเครื่องแล้วเปิดใหม่ เริ่มบูตใหม่จากแผ่นที่แน่ใจว่าไม่มีไวรัสคอมพิวเตอร์

3. การป้องกันฮาร์ดดิสค์นั้น ควรใช้ฮาร์ดดิสค์ที่ต่อแบบภายนอก โดยเมื่อเลิกใช้ก็ดึงปลั๊กออก ก็จะเป็นการป้องกันฮาร์ดดิสค์ได้บ้าง

4. อย่านำโปรแกรมคนอื่นที่ไม่แน่ใจว่าปลอดภัยจากไวรัสคอมพิวเตอร์มาใช้ แต่ถ้าจำเป็นต้องใช้ควรเช็คให้แน่ใจเสียก่อนว่าปลอดภัย

เพียงเท่านี้ก็จะเป็นการป้องกันไวรัสคอมพิวเตอร์ได้บ้างบางตัว

อาจารย์วิชิต ปุณวัตร์

ผู้เชี่ยวชาญพิเศษด้านระบบข้อมูลการพาณิชย์
กรมเศรษฐกิจการพาณิชย์

ไมโคร ช่วยให้คำจำกัดความ หรือความหมายของไวรัสคอมพิวเตอร์ว่ามันคืออะไร

อ.วิชิต ไวรัสคอมพิวเตอร์เป็นซอฟต์แวร์ที่เขียนขึ้น โดยมีเจตนาเพื่อให้มันเกิดความปั่นป่วน เกิดความผิดปกติไปจากงานที่ควรจะเป็น เจตนารมณ์ของผู้เขียนมี 2 ประเด็น คือ

1. การบ่อนทำลาย

2. นึกไม่ถึง แต่ร้อนวิชาอยากทดลองอะไรเล่น ซึ่งผู้เขียนส่วนใหญ่จะเป็นพวกนี้

จุดกำเนิดของไวรัสน่าจะมาจากต่างประเทศ ในบ้านเราอาจจะเกิดตัวใหม่ ๆ ขึ้นโดยผู้ที่ร้อนวิชา หรือต้องการทดสอบความสามารถ เอาไวรัสคอมพิวเตอร์คนอื่นมาแกะแล้วปรับปรุง

ขึ้นมาใหม่ ในกลุ่มนักศึกษา ในสถาบันการศึกษาต่าง ๆ อาจารย์ผู้สอนมีเจตนาดีนำไวรัสคอมพิวเตอร์มาให้ดูว่ามันทำงานอย่างไร เขาพัฒนากันอย่างไร ทำให้นักศึกษาอยากลองทำดู แต่ก็เป็นเพียงกลุ่มเล็ก ๆ เท่านั้น

ความคิดหนึ่งที่ทำให้เกิดไวรัสขึ้น คือ การป้องกันโปรแกรมที่ผู้ผลิตซอฟต์แวร์สร้างขึ้น ไม่ให้ผู้ใช้ที่ไม่ได้ซื้อซอฟต์แวร์ของเขา แต่พยายามก๊อบปี้โปรแกรมของเขาไปใช้ เขาจึงสร้างโปรแกรมไวรัสคอมพิวเตอร์ขึ้นมา โดยให้ทำลายตัวมันเองและโปรแกรมนั้นซึ่งเป็นการทำลายเฉพาะตัวเท่านั้น แต่ถ้านำซอฟต์แวร์ที่ผู้ผลิตมาใช้ตามปกติ โดยไม่ผิดเงื่อนไขที่ตั้งไว้ก็จะไม่ออกฤทธิ์ หรือแสดงอาการใด ๆ

ไมโคร การติดต่อของไวรัสคอมพิวเตอร์มาด้วยวิธีการใดบ้าง

อ.วิชิต ช่องทางที่ติดไวรัสคอมพิวเตอร์เข้ามาได้ พาหะนำเชื้อน่าจะเป็นพวกนักวิชาการ พวกครูบาอาจารย์ แม้กระทั่งคนทั่ว ๆ ไป ที่ไปมาต่างประเทศบ่อย ๆ มีความสนใจซอฟต์แวร์ต่าง ๆ ของต่างประเทศก็ก๊อบปี้มาโดยไม่ระวัง พาหะที่สำคัญอีกอย่างหนึ่งคือพวกนักศึกษาที่นำโปรแกรมนั้น ๆ มาใช้กันแพร่หลายกันทั่วไป และติดเข้าไปในหน่วยงานต่าง ๆ ในลักษณะการไปฝึกงานยังที่นั้น ๆ หรือเจ้าหน้าที่ของหน่วยงานนั้น ๆ บางคนไปเอาซอฟต์แวร์จากเพื่อน ๆ มาใช้โดยไม่ระวังในเรื่องไวรัสคอมพิวเตอร์ก็อาจติดไวรัสคอมพิวเตอร์ได้

ไมโคร ไวรัสคอมพิวเตอร์ตัวที่พบมีอะไรบ้าง มีอาการอย่างไร

อ.วิชิต ไวรัสคอมพิวเตอร์ตัวที่พบคือ (c) BRAIN เพียงตัวเดียว พอพบก็เลยวางมาตรการป้องกันไว้ อาการที่พบคือไฟล์หาย ซึ่งเป็นไฟล์ข้อมูล ถ้าเปิดไฟล์ดูก็ปรากฏว่าขาด ๆ วิ่น ๆ เวลาใช้โปรแกรมมันมีอาการเพี้ยน ๆ อยู่เรื่อย ๆ จึงทำการตรวจสอบว่ามันผิดปกติเพราะเหตุใด ภายหลังจึงแน่ใจว่าเป็นไวรัสคอมพิวเตอร์ที่ทำให้ข้อมูลผิดปกติ จากนั้นจึงได้นำซอฟต์แวร์ศิริราชเวอร์ชัน 2.0 มาตรวจสอบและแก้ไขไวรัสคอมพิวเตอร์ตัวนี้

ไมโคร ที่นี่มีมาตรการป้องกันหรือตรวจสอบอย่างไรบ้าง

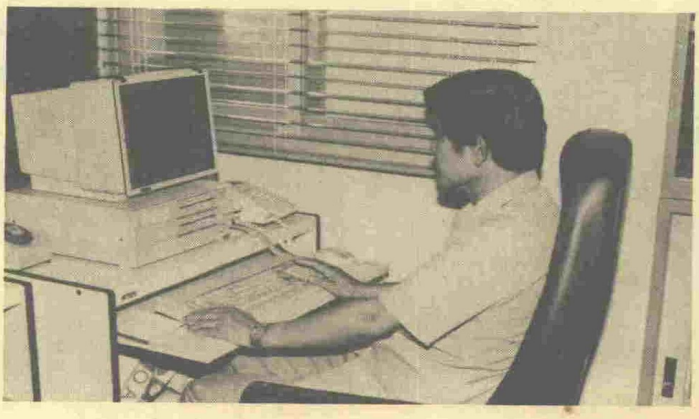
อ.วิชิต เรามีการตรวจสอบข้อมูลเราเสมอ มีการทดสอบก่อนจะส่งข้อมูลจริง มีการตรวจสอบผลงานของเรา นอกจากนั้นยังไม่ให้เจ้าหน้าที่สำส่อนในการนำโปรแกรมที่ไม่รู้จักหรือไม่แน่ใจมาใช้ แต่ถ้าจำเป็นจะใช้ต้องมีการตรวจสอบเสียก่อน ซึ่งเป็นการป้องกันไม่ให้เกิดการแพร่ระบาดและคิดว่าเป็นวิธีการที่ดีที่สุดแล้ว ถ้ามีการป้องกันมากกว่านี้เราต้องคำนึงถึงความสะดวกในการใช้งาน ความรวดเร็วในการทำงานด้วย ตลอดจนมีความผิดพลาดนั้นอาจจะเกิดได้ด้วยเหตุ 3 ประการคือ

1. ตัวบุคคลทำให้เกิดความผิดพลาด
2. เครื่องจักรผิดพลาด ซึ่งอาจจะเกิดการเสื่อมของตัวเครื่องจักรเอง
3. ซอฟต์แวร์ผิดพลาด รวมทั้งข้อมูลต่าง ๆ ด้วย

ไมโคร มีแหล่งให้คำปรึกษาเรื่องไวรัสคอมพิวเตอร์ที่ใดบ้าง

อ.วิชิต แหล่งให้คำปรึกษาเรื่องไวรัสคอมพิวเตอร์ให้ใช้สื่อมวลชน โดยเฉพาะหนังสือทางคอมพิวเตอร์เป็นแหล่งกลางจะดีที่สุด เพราะบ้านเราถ้าจะบอกว่ามีหน่วยงานอะไรรับผิดชอบโดยตรงตอบว่ายาก คนเก่งมักซุ่มทำงาน ถ้าไม่เรียกร้องจะไม่ปรากฏตัว บ้านเราอัศวินม้าขาวมีมาบ่อย ๆ แต่น่าเสียดายที่ไม่มีสถาบันรับผิดชอบเป็นเรื่องเป็นราว

สถาบันที่จะช่วยให้คำปรึกษาได้ เช่น สถาบันเทคโนโลยีพระนครเหนือ วิทยาเขตลาดกระบัง จุฬาลงกรณ์มหาวิทยาลัย มหาวิทยาลัยเกษตรศาสตร์ เป็นต้น แต่คิดว่าเรื่องเหล่านี้ควรใช้สื่อกลางหนังสือเป็นตัวพบปะกัน ต้องยอมรับว่าความหลากหลายของงานด้านคอมพิวเตอร์ได้เข้าไปแทรกแซงและพัฒนาในสาขาวิชาต่าง ๆ หลายประการ ในวิชาชีพหลายแขนง เพราะฉะนั้นเราต้องแยกกันเป็นผู้ชำนาญการคนละด้าน และคนที่จะเป็นตัวรวบรวมความคิดหรือเรื่องราวต่าง ๆ ได้ดีที่สุด คือ วารสารต่าง ๆ ซึ่งต้องให้การสนับสนุน



คุณไกรกร เศรษฐไกรกุล

วิศวกรไฟฟ้า สถาบันเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ไมโคร ไวรัสคอมพิวเตอร์คืออะไร

คุณไกรกร คือโปรแกรมชนิดหนึ่งที่สามารถติดต่อไปยังโปรแกรมต่าง ๆ ได้ แบ่งเป็น 2 ชนิดคือ

- บูตเซกเตอร์ไวรัส เช่น (c) BRAIN, T-2, FATERASER ฯลฯ
- ไฟล์ไวรัส เช่น sUMsDos

ไมโคร ไวรัสคอมพิวเตอร์ที่พบมีตัวใดบ้าง

คุณไกรกร ไวรัสที่พบมีทั้งหมด 5 ตัว คือ (c) BRAIN, T-2 หรือ TYPE-2, FATERASER, THREE WISE MEN และ sUMsDos

ไมโคร อาการและการทำงานของไวรัสแต่ละตัวเป็นอย่างไร

คุณไกรกร ตัวแรก (c) BRAIN พอเข้าไปก็จะทำการย้ายบูตเซกเตอร์ของจริงไปเก็บไว้ที่ ๆ หนึ่ง พร้อมกับตัวโปรแกรมจะมี 3 CLUSTER ที่เป็น BAD CLUSTER (เมื่อใช้ PC-TOOLS เรียกดู) ทำให้การทำงานของโปรแกรมช้าลง เพราะจะตรวจสอบข้อมูลตลอดเวลา จุดที่ทำให้เสียหายคือทำให้การเรียกข้อมูลช้า ไวรัสตัวนี้ไม่ติดฮาร์ดดิสค์

T-2 ลักษณะการทำงานคล้ายกับ (c) BRAIN

FATERASER ทำลายส่วนที่เรียกว่า FAT (File Allocation Table) ซึ่งเป็นตำแหน่งการชี้หาข้อมูลที่เก็บไว้ในแผ่นดิสค์ ทำให้โปรแกรมไม่สามารถเรียกข้อมูลได้ แต่ข้อมูลจริง ๆ ยังคงอยู่บนแผ่น

THREE WISE MEN เพิ่งเข้ามาทีหลัง การทำลายข้อมูลยังไม่แน่ใจ ไวรัสตัวนี้ใช้วิธีการก๊อบปี้ตัวเองเข้าไปในบูตเซกเตอร์ อาการยังไม่ทราบแน่ชัด

sUMsDos เป็นไวรัสประเภทไฟล์ไวรัส จะติดโปรแกรมที่เป็น .COM และ .EXE ซึ่งเป็นเอ็กซีคิวค์เทเบิลไฟล์ เมื่อเราใช้โปรแกรมที่มีไวรัสนี้ มันจะทำการย้ายตัวเองเข้าไปอยู่ในหน่วยความจำก่อน โดยจะเข้าไปอยู่ในลักษณะที่เรียกว่าเรสซิเดนต์โปรแกรม ต่อจากนั้นก็จะมีการเช็คตัวเองว่ามีอยู่ในหน่วยความจำหรือยัง ถ้ามีแล้วจะไม่เข้าไปอยู่อีก ต่อจากนั้นถ้ามีการนำโปรแกรมอื่นมารันบนเครื่อง ไวรัสตัวนี้ก็จะติดไปกับไฟล์ หรือโปรแกรมนั้น เมื่อรันโปรแกรมที่มีไวรัสครั้งแรกก่อนที่ไวรัสจะลงหน่วยความจำ จะมีการเช็คเวลาการตรวจสอบเวลามี 2 ลักษณะ คือ ตรวจสอบปี 1987 ถ้าเป็นปี 1987 จะไม่มีผลอะไรเกิดขึ้น แต่ถ้าไม่ใช่เครื่องจะมีอาการรวน การทำงานจะช้าและอาจจะมีช่องว่างกะพริบ ๆ อยู่บนจอ ต่อจากนั้นก็จะมาเช็คว่าเป็นวันศุกร์ที่ 13 หรือไม่ ถ้าพบว่าเป็นวันดังกล่าวจะทำเครื่องหมายไว้เพื่อเป็นการรับทราบ หลังจากนั้นถ้ามีการรันโปรแกรมอื่น ก็จะลบโปรแกรมนั้นทิ้งทันที

การติดของ sUMsDos นั้น ในโปรแกรมประเภท .COM จะติดเพียงครั้งเดียวแล้วจะไม่ติดอีก ส่วนโปรแกรมประเภท .EXE เมื่อติดแล้วจะมีการขยายขึ้นเรื่อย ๆ ตามจำนวนการใช้งานของโปรแกรมนั้น ซึ่งจะก่อให้เกิดปัญหาเรื่องดิสค์เต็ม ไม่สามารถรันโปรแกรมได้

ไมโคร เราจะมีวิธีการป้องกันไวรัสคอมพิวเตอร์อย่างไรบ้าง

คุณไกรกร การป้องกันโปรแกรมประเภทบูตเซกเตอร์ ให้เปิดเครื่องครั้งแรกด้วยแผ่นที่มีอยู่ประจำที่แน่ใจว่าปลอดภัยและไม่ใช่แผ่นของคนอื่นบูตเครื่อง จะป้องกันไวรัสประเภทบูตเซกเตอร์ได้ร้อยเปอร์เซ็นต์ แต่สำหรับไวรัสประเภทที่ติดมากับไฟล์ให้ใช้แผ่นปิดป้องกันการเขียนติดไว้ก็จะป้องกันได้ นอกจากนั้นอาจใช้โปรแกรมที่ตรวจเช็คไวรัสต่าง ๆ ตรวจสอบแผ่นที่ใช้เป็นประจำ ก็จะช่วยลดปัญหาเรื่องการทำลายข้อมูลของไวรัสได้บ้าง

ไมโคร มีอะไรจะแนะนำผู้ใช้เครื่องคอมพิวเตอร์เพื่อให้ปลอดภัยจากไวรัสคอมพิวเตอร์บ้าง

คุณไกรกร วิธีที่ดีที่สุดพยายามตรวจสอบโปรแกรมของตนเองหัดเป็นคนช่างสังเกต โดยเฉพาะแผ่นดิสค์ทุกแผ่นควรติดแผ่นป้องกันการเขียนไว้ให้หมด เพราะถ้ามีการเขียนอะไรเราก็จะได้ทราบทันที ถ้ามีความจำเป็นต้องเขียนข้อมูลลงไป ก็น่าจะมีการตรวจเช็คให้แน่ใจเสียก่อนว่าปลอดภัย การที่เราจะป้องกันไวรัสทุกตัวคงเป็นไปไม่ได้ เพราะไม่ทราบว่าตัวใหม่จะเข้ามาเมื่อไรอีก ก็ต้องแก้กันไปเรื่อย ๆ

จ.อ.ท. สานนท์ แก้วอบเชย

กรมสื่อสารทหารอากาศ
กองทัพอากาศ เจ้าหน้าที่ซ่อมบำรุง
คอมพิวเตอร์ กองปฏิบัติการซ่อมบำรุง
เครื่องจักรคำนวณ

ไมโคร ที่มาของไวรัสคอมพิวเตอร์ไม่ทราบว่าเกิดมาอย่างไร

คุณสานนท์ มาจากแนวความคิดของเกม โดยเขียนโปรแกรม 2 โปรแกรมมาสู้กัน โปรแกรมอีกฝ่ายหนึ่งก็จะพยายามลบโปรแกรมของอีกฝ่ายหนึ่งให้ได้ ถ้าอันไหนลบจนโปรแกรมของอีกฝ่ายหนึ่งทำงานไม่ได้ก็ชนะ ดังนั้นตัวโปรแกรมนั้น ๆ จึงต้องหาที่อยู่ใหม่ให้ได้มากที่สุด เมื่ออีกที่หนึ่งถูกลบ ตัวมันเองก็ยังสามารถรันได้อยู่ ต่อมามีผู้พัฒนาเป็นไวรัสคอมพิวเตอร์ และมีผู้นำประโยชน์นี้มาป้องกันการก๊อบปี้ซอฟต์แวร์ ถ้ามีการก๊อบปี้เมื่อใด โปรแกรมไวรัสก็จะออกมาทำงานตามที่ผู้เขียนต้องการในลักษณะการทำลายระบบ

ไมโคร ไวรัสคอมพิวเตอร์ที่พบมีตัวใดบ้าง

คุณสานนท์ ไวรัสคอมพิวเตอร์ที่พบมี (c) BRAIN, T-2 หรือ STUPID, Y.C.1.E.R.P และ sUMsDos ซึ่งทุกตัวเราสามารถแก้ได้แล้ว

ไมโคร อาการและการติดต่อของไวรัสแต่ละตัวเป็นอย่างไรบ้าง

คุณสานนท์ อาการและการติดต่อของไวรัสมีดังนี้

- (c) BRAIN การติดต่อเกิดจากการบูตแผ่นที่ติดลงในเครื่อง เมื่อเอาแผ่นอื่นมาใช้ก็จะติดทันที ไม่ว่าจะเป็นเพียงการไดเรคทอรีดูไฟล์ของแผ่นก็ตาม มันจะทำให้หน่วยความจำไป 7 KB เมื่อ Read หน่วยความจำของโปรแกรมเหล่านั้นจะพบข้อความของตัวมันอยู่คือ Welcome to the Dungeon (c) 1986 Brain โดยจะจองเนื้อที่ในดิสก์เราไว้ 3 CLUSTER (1 CLUSTER = 1024 BYTES) ถ้าติดมาก ๆ หรือนาน ๆ CLUSTER เสีย จะเพิ่มมากขึ้นเรื่อย ๆ ทำให้เนื้อที่ลดน้อยลง บางทีข้อมูลที่เก็บอยู่ถูกไวรัสไปทับ ข้อมูลเสียไป จะลบโปรแกรมไปทีละเล็กละน้อย เรียกโปรแกรมไม่ได้ แต่ (c) BRAIN จะไม่เข้าฮาร์ดดิสก์

- T-2 หรือ STUPID มีขนาดแค่ 1 KB การติดนั้นจะติดเมื่อกดรีบูตแผ่น มันจะทำลายแผ่น ลบ FAT ทำให้หาข้อมูลในแผ่นไม่ได้ เมื่อติดแล้วไปบูตกับเครื่องประเภทเอที จะทำงานไม่ได้ เครื่องจะเงียบไปเฉย ๆ ตัวนี้ไม่ลงฮาร์ดดิสก์

- Y.C.1.E.R.P ของญี่ปุ่น การทำงานคล้าย (c) BRAIN ทำให้เครื่องทำงานช้าลง ข้อมูลผิดพลาด เครื่องแฮง การติดต่อก็เช่นเดียวกับ (c) BRAIN ไม่ลงฮาร์ดดิสก์เช่นเดียวกัน

- sUMsDos ไวรัสตัวนี้ลงฮาร์ดดิสก์ และฟลอปปี้ดิสก์ทุกชนิด ไม่คำนึงถึงโอเอสที่รันอยู่ การติดจะติดมากับไฟล์หรือโปรแกรม ทำให้ไฟล์มีขนาดใหญ่ขึ้นเรื่อย ๆ เมื่อเรียกไฟล์ไวรัสจะมาทำงานและเพิ่มขนาดไฟล์ขึ้น จะติดมากับไฟล์ที่เป็น .COM และ .EXE ไฟล์ที่เป็น .COM จะติดอยู่ที่หัวไฟล์ จะติดเพียงครั้งเดียว ส่วนไฟล์ที่เป็น .EXE จะติดอยู่ที่ท้ายไฟล์ จะเพิ่มขนาดของไฟล์ขึ้นเรื่อย ๆ เมื่อรันโปรแกรมหรือไฟล์นั้น เมื่อไวรัสตัวนี้ทำงานไปนาน ๆ จะทำให้ฮาร์ดดิสก์หรือฟลอปปี้ดิสก์เต็ม ไม่สามารถใส่ข้อมูลได้อีก

ไมโคร ทราบว่าคุณสานนท์ผลิตวัคซีนการ์ดเพื่อตรวจสอบและทำลายไวรัสไว้ ไม่ทราบว่าหลักการทำงานของวัคซีนการ์ดทำอย่างไรบ้าง

คุณสานนท์ การทำงานของวัคซีนการ์ด เป็นฮาร์ดแวร์ที่ทำขึ้นให้ตรวจสอบไวรัสได้ทุกตัวที่มีในเมืองไทยปัจจุบัน โดยทำงานในระดับเดียวกันกับฮาร์ดแวร์ เมื่อมีซอฟต์แวร์ตัวใดสั่งเข้ามาทางไบออส และมีการส่งผ่านข้อมูล วัคซีนการ์ดจะก๊อบปี้ข้อมูลเหล่านั้นออกมาด้วย แล้วสุ่มตรวจสอบ เมื่อพบว่ามีการโหลดข้อมูลที่มีรหัสของไวรัสเข้ามาจะร้องเตือนขึ้นมาทางจอ ซึ่งเป็นวินโดว์ ถ้าเป็นไวรัสพวก (c) BRAIN, T-2 จะฆ่าทิ้งทันที แต่ถ้าเป็น sUMsDos จะหยุดการโหลดไฟล์นั้นทันที ไม่ให้รัน เพื่อไม่ให้ไวรัสลงไปในระบบ แล้วออกไปสู่ A> ใช้ไฟล์อีกไฟล์หนึ่งที่ชื่อ RTAF1 มาทำลาย sUMsDos นั้นเสีย การใช้วัคซีนการ์ดไม่ต้องเรียกจะทำงานควบคู่ไปกับการทำงานของเครื่องเลย

ไมโคร จะมีวิธีการป้องกันอย่างไรบ้างที่จะทำให้ปลอดภัยจากไวรัสคอมพิวเตอร์

คุณสานนท์ การป้องกันสามารถทำได้ดังนี้

1. การจะก๊อบปี้โปรแกรมอะไรของใคร ต้องตรวจสอบให้แน่ใจเสียก่อนว่ามีไวรัสหรือไม่

2. ถ้าเกิดสิ่งผิดปกติ ให้หยุดการทำงานของเครื่องก่อน แล้วสอบถามผู้รู้หรือดัมพ์ดูโปรแกรมว่าผิดปกติตรงไหน

3. ถ้าเป็นไวรัสที่ลงฮาร์ดดิสก์ เช่น sUMsDos ก็หยุดเรียกโปรแกรมที่ติดไวรัสนั้น แล้วหาโปรแกรมที่ทำลายไวรัสนั้นมาใช้

ผมอยากให้ทุกคนตรวจสอบแผ่นของตัวเอง อย่าให้ตัวเองเป็นสื่อของไวรัสไปส่งต่อให้คนอื่น ถ้าพบว่ามีไวรัสเกิดขึ้น ควรทำลายทิ้งเสีย ไม่ควรเก็บไว้ เพราะอาจจะพลาดนำมาใช้ก็จะเกิดความเสียหายได้

คุณสุรเดช มุขยางกูร

Microcomputer Dept. Manager
SCT. COMPUTER CO., LTD.

ไมโคร เคยพบปัญหาเกี่ยวกับเรื่องไวรัสคอมพิวเตอร์บ้างหรือไม่

คุณสุรเดช เคย แต่ไม่ใช่ที่นี่ เนื่องจากเราใช้ original program จากต่างประเทศ และเราก็มีวิศวกรคอยดูแลเครื่องอยู่ ซึ่งถ้าเกิดมีอาการผิดปกติขึ้นก็สามารถที่จะตรวจเช็คได้ ส่วนใหญ่จะเป็นปัญหาที่เกิดขึ้นกับลูกค้า แล้วเราก็ได้ช่วยแก้ปัญหานี้โดยแนะนำวิธีหรือโปรแกรมกำจัดไวรัสให้

ไมโคร ผลกระทบของไวรัสที่เกิดขึ้นกับลูกค้ามีมากน้อยอย่างไร

คุณสุรเดช ไม่มีผลกระทบอะไรมากนัก ส่วนใหญ่เมื่อเคยติดไวรัสแล้วก็จะเป็นเรื่องของความวิตกกังวลมากกว่า ซึ่งจะทำให้เสียเวลาในการตรวจเช็คมากขึ้น ส่วนในแง่ของความเสียหายของข้อมูลนั้นจะมีเพียงเล็กน้อยเท่านั้น เนื่องจากเมื่อเครื่องติดไวรัสแล้ว คอมพิวเตอร์จะแสดงอาการผิดปกติ ที่มาจากการกระทำของไวรัสคอมพิวเตอร์ให้ทราบ ดังนั้นจึงมีการแก้ไขและป้องกันได้ทัน

ไมโคร ผู้ใช้ควรปฏิบัติตนอย่างไร เพื่อเป็นการป้องกันการติดจากไวรัสคอมพิวเตอร์

คุณสุรเดช ควรจะมีการแบ็คอัพข้อมูลเป็นประจำ ไม่ควรใช้โปรแกรมจากแหล่งที่ไม่แน่ใจ

ไมโคร คอมพิวเตอร์ควรจะมีระบบป้องกันไวรัสหรือไม่

คุณสุรเดช การใช้ระบบป้องกันกับเครื่องนั้นผลที่เกิดขึ้นคือเครื่องจะทำงานช้าลง เพราะมันต้องคอยเช็คการอ่านและเขียนข้อมูล หรือเช็คขนาดของโปรแกรมก่อนและหลังการใช้งาน ซึ่งเป็นคุณสมบัติของโปรแกรมวัคซีนทั้งหลายที่มีในท้องตลาด ดังนั้นจึงควรพิจารณาในเรื่องของความจำเป็นด้วย

ไมโคร แหล่งที่มาของไวรัสน่าจะเป็นแหล่งไหนหรือคนประเภทไหนบ้าง

คุณสุรเดช การเกิดของไวรัสน่าจะเกิดจากความสอดรู้สอดเห็นของคนมากกว่า ถ้าลองสังเกตดูในระยะหลังมานี้คนที่อยู่ในวงการคอมพิวเตอร์ โดยเฉพาะอเมริกาจะเป็นเด็กทั้งนั้น ซึ่งเป็นคนที่มีการคิดอ่านค่อนข้างรวดเร็วและฉลาดมาก ๆ เพราะฉะนั้น ในบางครั้งจึงอาจจะคิดอะไรแปลก ๆ ใหม่ ๆ ขึ้นมาทำ เมื่อคิดเสร็จแล้วก็ขาดความยับยั้งชั่งใจ คือเค้ามองไม่เห็นผลกระทบที่จะเกิดขึ้น ดังนั้นจึงทำอะไรได้เรื่อย ๆ เพื่อความสนุก สังเกตง่าย ๆ โปรแกรมที่มีโปรเทคอยู่นั้น พวกที่ถอดโปรแกรมส่วนใหญ่ก็เป็นพวกเด็ก ๆ ซึ่งจริง ๆ แล้วนั้นไม่ได้มีจิตคิดร้ายอะไรต่อใคร แต่ทำขึ้นมาเพราะอยากจะลองวิชาเท่านั้นเอง

ไมโคร การระบาดของไวรัสจะมีผลกระทบอย่างไรบ้าง

คุณสุรเดช เราจะแยกได้ 3 กรณี คือ

- ในแง่ของผู้ซื้อหรือผู้ใช้งานนั้น ในปัจจุบันคอมพิวเตอร์ได้เข้าไปมีบทบาทในงานธุรกิจค่อนข้างมาก ข้อมูลต่าง ๆ นั้นก็จะใช้คอมพิวเตอร์ในการประมวลผล ซึ่งถ้าเกิดการทำลายข้อมูลโดยไวรัสคอมพิวเตอร์นี้ก็จะทำให้เกิดความเสียหายได้มาก

- ในแง่ของผู้ขาย จะมองได้ 2 กรณีคือ ดีและไม่ดี ซึ่งจะดีในแง่ผู้ใช้จะระวังการใช้ซอฟต์แวร์มากขึ้น และหันมาซื้อ original program มากขึ้น และไม่ดีในแง่คนจะหมดความเชื่อถือในซอฟต์แวร์ที่ไม่ใช่ original ซึ่งจะส่งผลกระทบต่อผู้ขายซอฟต์แวร์ที่ไม่ใช่ original ทั้งหลายในบ้านเรา และอาจส่งผลถึงผู้ขายคอมพิวเตอร์ด้วยว่า ผู้ใช้คอมพิวเตอร์อาจจะไม่ตัดสินใจที่จะนำคอมพิวเตอร์เข้ามาขยายงานเนื่องจากขาดความมั่นใจในการทำงานของคอมพิวเตอร์

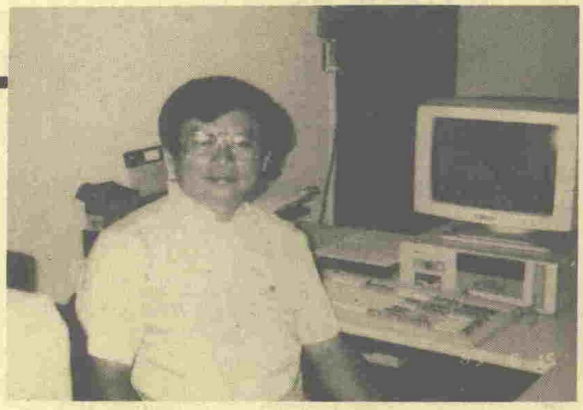
- ในแง่ภาพรวมของประเทศ ถ้าคนเกิดความกลัวทำให้มีการใช้คอมพิวเตอร์น้อยลง ทำให้การพัฒนาประเทศเป็นไปได้ช้า

ไมโคร แนวโน้มของการระบาดของไวรัสคอมพิวเตอร์จะเป็นอย่างไรต่อไป

คุณสุรเดช คิดว่าคงจะไม่หมดไปง่าย ๆ เนื่องจากเราไม่สามารถหยุดความคิดของคนได้ ตราบใดที่คนยังมีความคิดอยู่ก็อาจจะลองสิ่งแปลก ๆ ใหม่ ๆ ได้

ภก.อนุชิต จารุจุมพล

หัวหน้าแผนกเภสัชสถิติและแผนงาน กองเภสัชกรรม ฝ่ายการแพทย์และอนามัย การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย



ไมโคร คิดว่าไวรัสพวกใดที่มีอันตรายและสร้างปัญหาที่สุดในบ้านเราขณะนี้

ภก.อนุชิต พวกที่ทำลายข้อมูล หรือระบบงานใหญ่ ๆ ซึ่งไวรัสพวกนี้สามารถที่จะผ่านลงใน media ที่ใหญ่ ๆ ได้ อย่างเช่น ฮาร์ดิสก์ เป็นต้น

ไมโคร ไวรัสตัวใดที่เคยพบ และมีผลอย่างไร

ภก.อนุชิต พบเพียงตัวเดียวคือ Israeli ซึ่งจะมีผลทำให้การทำงานในฮาร์ดดิสก์หรือ File server ไม่ปกติหรือทำงานไม่ได้ การทำงานของเครื่องก็จะช้าลงเรื่อย ๆ ทำให้งานประจำอาจหยุดชงักลงได้

ไมโคร พบปัญหาที่เกิดจากไวรัสเมื่อไหร่และมีการแก้ไขอย่างไร

ภก.อนุชิต พบครั้งแรกประมาณ มี.ค. 32 จากนั้นก็ได้พยายามติดต่อสอบถามจากต่างประเทศ จึงทราบว่าเป็นไวรัสชนิดหนึ่ง แต่ก็ไม่มีซอฟต์แวร์ที่จะกำจัดไวรัสตัวนี้ในขณะนั้น จึงได้แก้ปัญหาเฉพาะหน้าโดยการเขียนโปรแกรม freeze ขึ้นเองซึ่งเป็นโปรแกรมที่ทำให้ไวรัสไม่ทำงานจากนั้นก็เขียนโปรแกรม check และ pure ในการตรวจและรักษา และต่อมาก็ได้รวมเอาคุณสมบัติของ check และ pure สร้างเป็นโปรแกรม pure2

ไมโคร ไวรัสชนิดนี้ทำให้เกิดความเสียหายในบ้านเราอย่างไรบ้าง

ภก.อนุชิต ใน กฟผ. เองก็ได้ผลกระทบเช่นกันแต่ที่เห็นชัดคือ สถาบันการเงิน โรงงาน และรัฐวิสาหกิจบางแห่งได้รับผลกระทบนี้ ทำให้เกิดความเสียหายคิดเป็นมูลค่าประมาณได้เป็นหลักล้านบาทต่อเดือน ซึ่งเป็นเหตุการณ์ที่เกิดขึ้นช่วงต้นปีนี้เอง

ไมโคร สถานการณ์ปัจจุบันในบ้านเราในการระบาดของไวรัสเป็นอย่างไร

ภก.อนุชิต ในช่วงนี้เหตุการณ์ดีขึ้นแล้ว เนื่องจากในช่วงที่มีการระบาดในหน่วยงานใหญ่ ๆ ตอนนั้นเราได้ช่วยแก้ปัญหาจากโปรแกรมกำจัดไวรัสที่คิดขึ้นเองดังที่กล่าวมาแล้ว ซึ่งช่วงนั้นก็ได้มีหน่วยงานจากแหล่งต่าง ๆ ทั้งภาครัฐบาลและเอกชน มาติดต่อให้เราช่วยเหลือ

ไมโคร เนื่องจากปัจจุบันมีโปรแกรมแก้ไวรัสมากขึ้น มีข้อแนะนำในการใช้โปรแกรมเหล่านี้อย่างไรบ้าง

ภก.อนุชิต ปัญหาที่ค่อนข้างสำคัญที่เคยประสบในการทดลองใช้งานโปรแกรมกำจัดไวรัสในบูตเซกเตอร์ในโหมดการ protect คือถ้าเป็นดิสเกตต์ที่มีความจุต่างขนาดกับ 360 KB. จะทำให้ดิสเกตต์นั้นไม่สามารถใช้งานได้อีก เนื่องจากฟอร์แมตในบูตเซกเตอร์ของดิสเกตต์ที่มีความจุต่างกันจะไม่เหมือนกันทำให้เกิดความผิดพลาดในการ protect ในส่วนของบูตเซกเตอร์นี้ได้ ซึ่งเป็นข้อที่ควรจะระวังให้มาก ๆ

คุณสุรเมธ สัจจอิสริวุฒิ

นักศึกษาทดลองวิจัยปริญญาโท
คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยี
พระจอมเกล้า เจ้าคุณทหาร ลาดกระบัง

ไมโคร ไวรัสคอมพิวเตอร์คืออะไรตามความคิดเห็นของคุณสุรเมธ

คุณสุรเมธ ไวรัสคอมพิวเตอร์ คือโปรแกรมซึ่งออกแบบมาเพื่อจุดประสงค์ในการกลั่นแกล้งผู้อื่น ไม่ว่าจะเป็นรูปแบบไหนก็ตาม แล้วปล่อยออกมาให้ระบาดมากที่สุดเท่าที่จะเป็นไปได้ การระบาดของไวรัสจะเป็นไปเรื่อย ๆ ตราบใดที่มีเครื่องคอมพิวเตอร์ใช้อยู่ในโลก

ผู้ที่จะเขียนโปรแกรมไวรัสคอมพิวเตอร์ได้ ต้องมีความเกี่ยวข้องกับฮาร์ดแวร์มาก อย่างน้อยต้องรู้ในระดับการเขียนโปรแกรมชั้นสูง รู้ระบบโอเอสของเครื่องนั้น ๆ ซึ่งเป็นเรื่องยากและโปรแกรมไวรัสที่ดีต้องเขียนด้วยภาษาและแอสเซมบลี

ไมโคร อยากทราบว่าไวรัสคอมพิวเตอร์ที่พบมีตัวใดบ้าง การติดต่อติดได้ด้วยวิธีการใด

คุณสุรเมธ ไวรัสตัวแรกสุดที่พบคือ (c) BRAIN ตัวนี้ติดง่ายมาก เข้ามาในเมืองไทยเมื่อปีที่แล้วนี้เอง การติดต่อจะเข้าไปอยู่ในบูตเซกเตอร์ เพียงเรียกไดเรคทอรีดูก็ติดแล้ว เมื่อตัวนี้เข้ามาจึงได้เริ่มเขียนโปรแกรมวัคซีนศิริราชขึ้นเพื่อแก้ไวรัสตัวนี้ โดยเขียนร่วมกับพี่ชาย ไวรัสตัวต่อมาที่เจอคือ T-2 การติดต่อจะเกิดขึ้นได้เมื่อกด [Ctrl], [Alt] และ [Del] จะติดทันที ถ้าติดแล้วผลบูตแผ่นครบ 5 ครั้ง พอครั้งที่ 6 มันจะทำการฟอร์แมตตัวเองทิ้งทั้ง FAT ทำลายทั้งเซกเตอร์ โดยจะเรียกไบออสให้ทำการฟอร์แมตใหม่ ข้อมูลเรียกกลับมาได้แต่ลำบาก ตัวมันเองอยู่ในบูตเซกเตอร์ ไวรัสตัวต่อมาที่พบคือ FATERASER สันนิษฐานว่าพัฒนาไปเป็น T-2 การทำงานเหมือน T-2 จะติดในบูตเซกเตอร์ ทำงานเหมือนกับ (c) BRAIN แต่หลักการของ (c) BRAIN ดีกว่า และตัวสุดท้ายที่เจอคือศุกร์ที่ 13 หรือ sUMsDos หรือ ADS หรืออิสรา-เอลไวรัส ตัวมันจะติดไปกับไฟล์ที่เป็น .COM และ .EXE แต่ไม่ติดไฟล์ที่เป็น COMMAND.COM ซึ่งตัวนี้ผมได้กำลังทำโปรแกรม SIRIRAJ RELEASE 4 ขึ้นแก้ไขและตรวจสอบ

ไมโคร โปรแกรมวัคซีนศิริราชที่คุณสุรเมธสร้างขึ้นมานั้นไม่ทราบว่าป้องกันไวรัสตัวใดได้บ้าง

คุณสุรเมธ โปรแกรมวัคซีนที่ใช้ป้องกันได้มี (c) BRAIN และศุกร์ที่ 13 ตัวอื่นป้องกันไม่ได้ เพราะหลักการของไวรัสตัวที่เหลือมันจะตรวจสอบทั้งบูตเซกเตอร์ ป้องกันไม่ได้อยู่แล้ว ถ้าเราป้องกันก็คือเขียนให้เหมือนกันหมด ซึ่งก็เป็นการเขียนไวรัสให้ผู้ใช้นั่นเอง ตัวที่ร้ายที่สุดน่าจะเป็น T-2 เพราะมันจะฟอร์แมต FAT ของเราทิ้ง ข้อมูลของเราก็หายไปด้วย เรียกข้อมูลกลับมาได้แต่ยุ่งยากมาก

ผมขอบอกว่าโปรแกรมศิริราชที่ผมได้ทำขึ้นนั้นไม่ได้ขาย บริจาคให้ผู้ใช้ฟรี โดยไม่คิดมูลค่า แต่มีผู้นำไปก็อบปี้ขาย ซึ่งผิดวัตถุประสงค์ของผมอันเป็นการซ้ำเติมคนที่ประสบปัญหาเรื่องไวรัสอยู่แล้ว

ไมโคร มีวิธีการอะไรที่ตรวจสอบว่าเครื่องคอมพิวเตอร์ของเราติดไวรัส

คุณสุรเมธ หน่วยความจำของเครื่องหายไปโดยไม่ทราบสาเหตุ หรือเครื่องคอมพิวเตอร์มีอาการแปลกไปจากเดิม เช่น มีการทำงานช้าลง เป็นต้น

ถ้าไม่ต้องการให้ติดไวรัส ควรใช้โปรแกรมของตัวเองคนเดียว ตัดจากโลกภายนอก ซึ่งเป็นไปไม่ได้ ดังนั้น ต้องมีการตรวจแผ่นดิสก์ที่นำมาใช้ว่ามีไวรัสอยู่หรือไม่สำหรับแผ่นโปรแกรมใหม่ ๆ ที่นำมาใช้

ไมโคร ในระบบ LAN ที่ใช้อยู่มีโอกาสติดไวรัสหรือไม่

คุณสุรเมธ เทอร์มินัลที่ต่อกับเมนเฟรมหรือมินิคอมพิวเตอร์นั้น ไวรัสติดไม่ได้ การที่เราทำเทอร์มินอล คือ การที่เราทำการดึงข้อมูลออกมาดูเฉย ๆ การดึงข้อมูลไป ข้อมูลนั้นจะถูกเอาไปโพรเซส แต่ไม่ได้ถูกเอาไปเอ็กซีคิวต์ บนเมนเฟรมไม่ได้รันตามคำสั่งที่ส่งไป แต่จะเอาข้อมูลของเราไปวิเคราะห์ คือมันมีโปรแกรมของมันเองอยู่แล้ว ทำให้เมนเฟรมติดยากมาก นอกจากนั้นระบบความปลอดภัยของเมนเฟรมและมินิสูงมาก ถ้าจะใช้ต้องมีรหัสผ่าน และอื่น ๆ อีกหลายอย่าง ถ้าคุณผ่านได้และเอาไวรัสเข้าไปเขาก็รู้ว่าใครทำ

ไมโคร โปรแกรมไวรัสคอมพิวเตอร์สามารถเขียนให้ทำลายฮาร์ดแวร์ของเครื่องได้หรือไม่

คุณสุรเมธ เป็นไปได้เช่นกัน แต่จะสามารถทำลายเฉพาะเจาะจงกับฮาร์ดแวร์บางชนิดเท่านั้น ซึ่งจะต้องเข้าใจในระบบของฮาร์ดแวร์และคำสั่งที่จะมีผลบังคับให้ฮาร์ดแวร์ทำงานไม่สัมพันธ์กัน ทำให้เกิดการชำรุดได้ เช่น การทำให้ดิสก์ไดรฟ์เสียเนื่องจากการบังคับให้หัวอ่านทำงานไม่สัมพันธ์กัน หรือการทำให้จอภาพไหม้โดยเฉพาะของโมโนโครมที่ใช้กับเฮอร์คิวลิสการ์ดโดยการโปรแกรมไอซีเบอร์ 6845 เป็นต้น ซึ่งคิดว่าไม่ค่อยมีใครได้ทำกันเนื่องจากเฉพาะเจาะจงเกินไปและทำให้การระบาดเป็นไปได้น้อย

คุณเจริญพล ฉลองความดี

Managing Director

สำนักงานมหาจักรกฎหมาย

ไมโคร บทลงโทษทางกฎหมายเกี่ยวกับเรื่องของไวรัสคอมพิวเตอร์จะเป็นไปได้หรือไม่

คุณเจริญพล เป็นไปได้เช่นกันเนื่องจากเป็นเรื่องของการเจตนาเป็นหลัก โดยขึ้นอยู่กับว่าถ้าเจตนานั้นมีมูลเหตุชักจูงใจที่จะทำให้ใครได้รับความเสียหาย ซึ่งในเรื่องประมวลกฎหมายอาญาได้เขียนไว้ชัดเจนว่า การที่ทำให้ทรัพย์สินของใครเสียหาย โดยมุ่งเจตนาที่ก่อให้เกิดความเสียหายนั้น ก็จำต้องได้รับโทษไป

ไมโคร ในกรณีที่ไม่ได้มีเจตนา อย่างเช่น เราทดลองโปรแกรมไวรัสในดิสเกตต์แผ่นหนึ่ง แล้วมีเพื่อนนำไปใช้โดยไม่รู้ทำให้เกิดการระบาดไป จะมีผลอย่างไรบ้าง

คุณเจริญพล ลักษณะอย่างนี้จะเข้าสู่เรื่องทางแพ่ง คือ เป็นการประมาทเลินเล่อ ซึ่งเจ้าของน่าจะรู้อยู่แล้วว่าเป็นสิ่งที่จะทำให้เกิดความเสียหายแก่ผู้อื่นได้ ซึ่งควรจะมีการป้องกันและระวังในเรื่องนี้ แต่มิได้กระทำ ซึ่งก็จะเข้าสู่ตัวบทกฎหมายที่เป็นการประมาทเลินเล่อดังกล่าว

ไมโคร เราสามารถออกกฎหมายให้ถือว่า ไวรัสคอมพิวเตอร์เป็นสิ่งอันตราย ห้ามมีไว้ครอบครองได้หรือไม่

คุณเจริญพล น่าจะได้ โดยกฎหมายที่จะออกมาบังคับใช้นั้นก็จะต้องมีขั้นตอน ซึ่งจะต้องอธิบายเรื่องนี้ให้คนที่จะตรากฎหมายเข้าใจเสียก่อน คนที่จะเสนอนั้นน่าจะเป็นหน่วยงานที่รับผิดชอบในเรื่องนี้ เช่น กระทรวงวิทยาศาสตร์ เป็นต้น

ไมโคร ถ้าบริษัทผู้ผลิตซอฟต์แวร์ป้องกันการก๊อบปี้ โดยใช้ไวรัสแฝงเข้าไปจะเป็นเรื่องที่ถูกกฎหมายหรือไม่

คุณเจริญพล เราต้องมาดูว่าเป็นการป้องกันที่เกินกว่าเหตุหรือไม่ เช่น ถ้าป้องกันในลักษณะเช่นนี้แล้ว ทำให้ข้อมูลของคนอื่นเสียหาย แล้วระบาดไปได้ ซึ่งจะมีผลกระทบต่อส่วนรวมก็เป็นเรื่องที่ไม่ถูกกฎหมาย แต่ในกรณีที่ป้องกันโดยทำลายเฉพาะแผ่นของตัวเองก็น่าจะกระทำได้

ไมโคร ไม่ทราบว่าที่บริษัทของคุณเจริญพลเองเคยประสบปัญหาไวรัสคอมพิวเตอร์บ้างหรือไม่

คุณเจริญพล ไม่เคย เพราะเราไม่ได้ใช้โปรแกรมจากภายนอก เราจ้างโปรแกรมเมอร์ให้เขียนโปรแกรมขึ้นใช้งานเอง ซึ่งในลักษณะนี้ก็เป็นวิธีหนึ่งที่จะช่วยป้องกันไม่ให้ไวรัสมาติดได้เช่นกัน

อาจารย์พงษ์ ทรงพงษ์

ภาควิชาฟิสิกส์
จุฬาลงกรณ์มหาวิทยาลัย

ไมโคร ไวรัสคอมพิวเตอร์ที่พบมีตัวใดบ้าง

คุณพงษ์ ไวรัสตัวแรกที่พบไม่ทราบว่าชื่ออะไร อาการที่แสดงคือเมื่อบูตเครื่องแล้ว หน่วยความจำลดลงเหลือแค่ 639 KB แต่ลบทิ้งหมด ตัวนี้จะติดไปตามบูตเรคอร์ด ซึ่งตัวนี้ไม่ร้ายแรงนัก เพราะมันไม่เข้าไปยุ่งเกี่ยวกับข้อมูลอันใด ต่อมาพบไวรัสคอมพิวเตอร์ที่เรียกว่า (c) BRAIN ก็ไม่น่าเป็นห่วงเท่าไรนัก เพราะมันจะแพร่ไปในบูตเรคอร์ดเท่านั้น ถ้าเราบูตเครื่องด้วยแผ่นที่แน่ใจว่าไม่มีไวรัสคอมพิวเตอร์ตัวนี้ก็จะไม่เป็นไร ส่วนตัวที่พบหลังสุดคือ sUMsDos VIRUS ซึ่งจะติดไปตามโปรแกรมที่เป็น .COM และ .EXE ตัวนี้น่ากลัวมาก เพราะมันเพิ่มตัวเองเข้าไปในโปรแกรมได้ ในโปรแกรมที่เป็น .COM จะเพิ่มเพียงครั้งเดียวก็ยังไม่เท่าไร แต่ในโปรแกรมที่เป็น .EXE เพิ่มเป็นสิบ ๆ หนก็ยังเคยเจอ เมื่อมันเพิ่มตัวมาก ๆ จะทำให้หน่วยความจำของดิสก์เต็ม ไม่สามารถทำงานของโปรแกรมนั้นได้

ไมโคร การแพร่กระจายของไวรัสเกิดขึ้นได้อย่างไรบ้าง

คุณพงษ์ การแพร่กระจายทางหนึ่ง คือ มาจากตามร้านคอมพิวเตอร์ต่าง ๆ ที่เขาให้ก๊อบปี้โปรแกรม ควรจะมีการตรวจสอบโปรแกรมที่ใช้ก๊อบปี้ให้ลูกค้าว่ามีไวรัสคอมพิวเตอร์อยู่หรือเปล่า ถ้ามีก็ไม่ควรจะปล่อยโปรแกรมดังกล่าวออกไป แต่ก็ปล่อยออกไปเรื่อย ๆ ทำให้เกิดการแพร่ระบาดออกไปเรื่อย ๆ ตัวนี้หมดไปตัวใหม่ก็โผล่ขึ้นมาอีก

นอกจากการแพร่ระบาดของไวรัสคอมพิวเตอร์จะมาจากร้านคอมพิวเตอร์แล้ว ไวรัสคอมพิวเตอร์พวกที่ติดไปกับไฟล์อาจจะติดไปทางโมเด็ม หรือทางพวกแล็ปลิงค์ต่าง ๆ ก็ได้ เพราะถ้ามันติดอยู่บนโปรแกรมที่เป็น .EXE แล้วมันก็คงส่งต่อไปได้ตลอด ไม่ว่าเราจะส่งไปทางใด

ไมโคร ไม่ทราบว่าที่นี่มีวิธีการป้องกันไวรัสคอมพิวเตอร์อย่างไรบ้าง

คุณพงษ์ การป้องกัน sUMsDos VIRUS เราทำโดยใช้ PCTOOLS ตรวจสอบดิสเกตต์ทุกแผ่นว่าโปรแกรมทุกโปรแกรมนั้นมีคำว่า sUMsDos อยู่หรือเปล่า ไม่ให้บูตเครื่องโดยใช้แผ่นดิสก์จากภายนอก ให้บูตจากฮาร์ดดิสก์ของตัวเครื่องเอง ก็สามารถป้องกันไวรัสที่ติดมากับบูตเซกเตอร์

ศาสตราจารย์ ดร.ไพรัช ธัชยพงษ์

ผู้อำนวยการ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติเทคโนโลยีและการพลังงาน กระทรวงวิทยาศาสตร์

ไมโคร มีความคิดเห็นเกี่ยวกับไวรัสคอมพิวเตอร์อย่างไร

ดร.ไพรัช จะสังเกตได้ว่า จากเทคนิคการเขียนและการทำงานของมัน เป็นบทพิสูจน์อย่างหนึ่งว่าซอฟต์แวร์คอมพิวเตอร์นั้นมีความคล่องตัวมาก คือ ใครจะเอาไปทำให้เกิดผลดีหรือผลร้ายได้ง่าย

ไมโคร มีแหล่งหน่วยงานหรือสถาบันไหนที่มีการศึกษาเรื่องไวรัสนี้

ดร.ไพรัช ที่ลาดกระบังเราเองก็มีการศึกษาเรื่องนี้อยู่ แต่ก็ยังไม่ได้เผยแพร่ออกไป โดยผมเองก็มีการประชุมกับนักศึกษาและนักวิจัยที่ลาดกระบังว่าไวรัสมันคืออะไร ทำงานอย่างไร และมีผลร้ายอย่างไร

ไมโคร เราจะเผยแพร่ให้ประชาชนทั่วไปทราบได้อย่างไรเกี่ยวกับไวรัสคอมพิวเตอร์

ดร.ไพรัช คิดว่าเป็นหน้าที่ของ NECTEC ด้วย ซึ่งจะทำการวิจัยและจัดสัมมนาขึ้น ซึ่งปรากฏว่าเป็นสิ่งที่ดีที่หลายบุคคลในวงการคอมพิวเตอร์ตื่นตัว และมีการจัดสัมมนาอภิปรายกันมากขึ้น

ไมโคร การวิจัยศึกษาในเรื่องของไวรัสจะส่งผลอย่างไรบ้าง

ดร.ไพรัช มีบางท่านบอกผมว่าให้ระวังการวิจัย เผยแพร่เรื่องไวรัสมากจะทำให้มีคนเขียนไวรัสมากขึ้น ซึ่งคิดว่าอาจจะมีผลบ้าง แต่ถ้าเราทำให้มันกระจ่างและเข้าใจมันจะดีกว่าที่จะไม่รู้ว่ามันคืออะไร ทำงานอย่างไร ซึ่งจะมีผลต่อการหาทางแก้ไขต่อไป

ไมโคร สิ่งที่จะเป็นข้อแนะนำสำหรับผู้ที่เกี่ยวข้องกับคอมพิวเตอร์มีอย่างไรบ้าง

ดร.ไพรัช ที่น่าเป็นห่วงคือ ในหน่วยงานใหญ่ ๆ ซึ่งควรที่จะเริ่มทำความเข้าใจและระวังในเรื่องนี้ โดยเฉพาะการแลกเปลี่ยนข้อมูลหรือโปรแกรมกันบ่อย ๆ

คุณนพดล เลิศอัศววิวัฒน์

Asst. Mkt. Tech. Sup. Manager
SAHAVIRIYA SYSTEM CO., LTD.

ไมโคร ไวรัสตัวใดที่พบบนเครื่อง MAC บ้าง

คุณนพดล ที่พบบนเครื่อง MAC ในตอนนี้นั้นมีทั้งหมด 6 ชนิด แต่ที่พบในบ้านเรานั้นมีเพียงตัวเดียวคือ ไวรัส nVir ตอนแรกก็ทราบข่าวว่ามีการระบาดของไวรัสบนเครื่อง PC ต่อมาภายหลังก็พบอาการประหลาด ๆ บนเครื่อง MAC ประกอบกับพอดีทางเมืองนอกได้ส่งโปรแกรมเช็คไวรัสมาให้ โปรแกรมชื่อ Interferon ซึ่งหลังจากเช็คดูแล้ว ก็พบว่ามีไวรัสจริงเกิดขึ้นจริง ๆ บนเครื่อง MAC ของเรา

ไมโคร ลักษณะการติดต่อของไวรัสตัวนี้เป็นอย่างไร

คุณนพดล มันจะผ่านเข้าสู่ในระบบ System เมื่อเรารันแอพพลิเคชั่นที่มีไวรัสนี้ หลังจากนั้นทุกโปรแกรมที่เรารันก็จะติดไปด้วย โดยจะติดเฉพาะโปรแกรมที่สามารถรันได้เท่านั้น ส่วนดาต้าไฟล์จะไม่ติด และสามารถผ่านเข้าสู่ฮาร์ดดิสค์ได้ ในเรื่องของ LAN นั้นก็สามารถติดต่อได้เช่นกัน

ไมโคร แหล่งที่มาของไวรัส nVir นี้มาจากแหล่งใด

คุณนพดล ส่วนใหญ่การติดไวรัสจะได้มาจากโปรแกรมที่เป็น Public domain หรือ Shareware โดยที่อาจติดมาจากโปรแกรมที่ลูกค้านำมาจากเมืองนอก แล้วมาใช้เครื่องของเรา

ไมโคร อาการของไวรัส nVir เป็นอย่างไร

คุณนพดล จะทำให้โปรแกรมที่ใช้รันเสียได้ ซึ่งจะรันได้ครั้งเดียว จะสังเกตได้จากเสียงประหลาดอื่นที่ดังขึ้นมา นอกจากเสียง Beep ของ System

ไมโคร การกำจัดไวรัส nVir ทำอย่างไร

คุณนพดล เนื่องจากโปรแกรม Interferon นั้น จะเอาไฟล์ที่ติดไวรัสของเราออกไปด้วย เราจึงเขียนโปรแกรมขึ้นใหม่โดยเช็คไวรัสเมื่อพบแล้วจะกำจัดเฉพาะไวรัสออก ส่วนตัวโปรแกรมก็ยังสามารถใช้งานได้อยู่

ไมโคร การป้องกันไวรัสชนิดนี้ควรทำอย่างไร

คุณนพดล พยายามอย่าให้มันเข้าไปใน System ได้ ควรใช้โปรแกรมที่ได้ผ่านการตรวจสอบว่าปราศจากไวรัสแล้วเท่านั้น และไม่ควรนำโปรแกรมจากแหล่งที่ไม่น่าเชื่อถือมารันบนเครื่องเรา